

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-281022
(P2002-281022A)

(43)公開日 平成14年9月27日 (2002.9.27)

(51)Int.Cl.
H 0 4 L 9/22

識別記号

F I
H 0 4 L 9/00

テマコード(参考)
6 5 5 5 J 1 0 4

審査請求 未請求 請求項の数10 O L (全 8 頁)

(21)出願番号 特願2001-79463(P2001-79463)

(22)出願日 平成13年3月19日 (2001.3.19)

(71)出願人 501109116

有限会社 ネットイメージ
東京都江東区青海2-45 タイム24ビル4
階

(72)発明者 斎藤 兆古

東京都あきる野市山田778-12

(72)発明者 黄 富石

東京都港区海岸3-9-40-1304

(74)代理人 100109726

弁理士 園田 吉隆 (外1名)

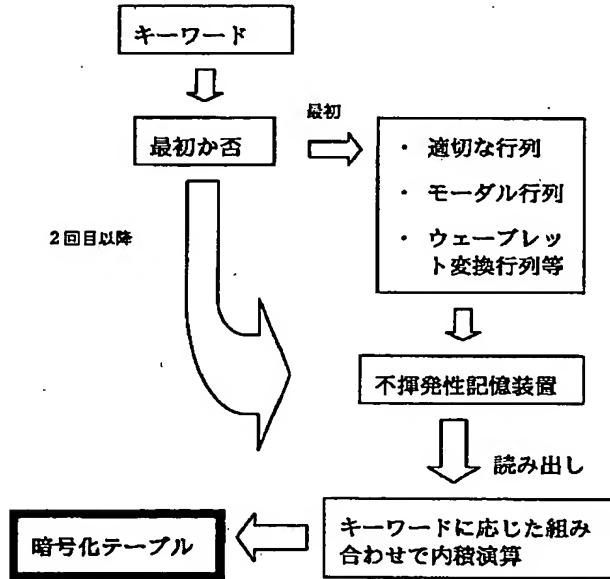
Fターム(参考) 5J104 AA18 JA04 NA01 NA14 PA02
PA07

(54)【発明の名称】 情報の暗号化／解読方法と同システム

(57)【要約】 (修正有)

【課題】 デジタル計算機を前提とするインターネットや携帯電話等の情報送受信機器と高度な秘匿性を要する大量の情報を格納するデジタル計算機システムにおいて、ユーザが意識することなく、文字、画像、音声等の情報を暗号化し、ユーザが意識することなく、暗号化された情報を解読し、原情報を再生するセキュリティシステムを提供する。

【解決手段】 ユーザの識別情報、例えば、住所、氏名、生年月日、電話番号、ID番号、パスワード、e-mailアドレス等や、ユーザが独自に決めた識別情報を単独、若しくは複数組み合わせたキーワードを用いて自動的に暗号化テーブルを生成し、ユーザの所有する情報の自動暗号化、および暗号化された情報の自動解読を行う方法であって、個人情報や企業・組織情報の漏洩を削減するセキュリティ高度化法とその装置である。



【特許請求の範囲】

【請求項1】 ユーザに固有の情報と、ユーザが任意に設定する識別情報の中から選択された1つ以上を組み合わせてキーワードを作成し、該キーワードを用いて少なくとも1つの逆行列を有する適切な行列 (well posed matrix) である暗号変換行列を設定し、前記デジタルデータと該暗号変換行列とを積算することによってデジタルデータを暗号化するデータの暗号化方法。

【請求項2】 前記ユーザに固有の情報は、ユーザの住所、氏名、生年月日、電話番号、ID番号、パスワード、e-mailアドレスの内の少なくとも1つを含むものである請求項1に記載の暗号化方法。

【請求項3】 前記のキーワードは、ユーザが独自に決めた任意の組み合わせを選択可能であり、ユーザが独自に決めた任意の日時で自動的に更新可能であることを特徴とする請求項1又は2のいずれかに記載の方法。

【請求項4】 ユーザが意識することなく、キーワードを用いて自動的に暗号化行列を生成し、ユーザの所有する情報を自動的に暗号化することを特徴とする請求項1ないし3のいずれかに記載された方法。

【請求項5】 前記暗号変換行列は、单一、若しくは複数の適切な行列の固有ベクトルから生成される单一、若しくは複数のモーダル行列を組み合わせて自動的に生成されたものであり、データを自動的に暗号化することを特徴とする請求項1ないし4のいずれか記載された方法。

【請求項6】 前記暗号変換行列は、キーワードを用いて、单一、若しくは基底関数の異なる複数のウェーブレット変換行列を用いて自動的に暗号化行列を生成し、ユーザの所有する情報を自動的に暗号化することを特徴とする請求項1ないし4のいずれかに記載の方法。

【請求項7】 前記暗号変換行列は、单一、若しくは複数の適切な行列の固有ベクトルから生成される单一、若しくは複数のモーダル行列と、キーワードを用いて作成した、单一、若しくは基底関数の異なる複数のウェーブレット変換行列を組み合わせて作成したものであることを特徴とする請求項1ないし4のいずれかに記載の方法。

【請求項8】 階層ごとに暗号変換行列を設定し、データを当該階層の暗号変換行列及び当該層より下のすべての階層の変換行列を用いて重疊的に変換することにより、上位の階層の属するユーザには当該層及び下位の階層の暗号化データは読めるが、上位の階層の暗号化データは読めないことにした階層化暗号化方法。

【請求項9】 ユーザに固有の情報と、ユーザが任意に設定する識別情報の中から選択された1つ以上を組み合わせてキーワードを作成し、該キーワードを用いて少なくとも1つの逆行列を有する

適切な行列 (well posed matrix) である暗号変換行列の逆行列を求め、

暗号化されたデジタルデータと該暗号変換行列の逆行列とを積算することによって暗号化されたデジタルデータを解読するデータの解読方法。

【請求項10】 ユーザに固有の情報と、ユーザが任意に設定する識別情報の中から選択された1つ以上を組み合わせてキーワードを作成部と、該キーワードを用いて少なくとも1つの逆行列を有する適切な行列 (well pos

ed matrix) である暗号変換行列を設定部とを有して、前記デジタルデータと該暗号変換行列とを積算することによってデジタルデータを暗号化するデータの暗号化手段と、前記適切な行列の逆行列を算出する逆行列算出部と、暗号化されたデジタルデータと該逆行列とを積算することによって暗号化されたデジタルデータを解読するデータの解読手段とを有するデータの暗号化解読システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタルデータの暗号化手法に関するものであり、より具体的には、インターネットや携帯電話等の情報通信機器や、大量の情報を格納するデジタル計算機システムにおいて、個人情報や企業・組織情報の漏洩の可能性を低減して情報のセキュリティを高度化するための暗号化方法、当該暗号化された情報を解読する方法、および、これらの方法を実施するシステムに関するものである。

【0002】

【従来の技術および発明が解決しようとする課題】 インターネットや携帯電話等を通じた情報通信と、大量の情報を格納するデジタル計算機システムにおいては、個人情報や企業・組織情報を適切に保護して情報の秘匿性を確保することが必須である。この種のセキュリティ問題を解決する方法の1つとして、暗号化手法がある。

【0003】 しかし、計算機で暗号化された情報は、基本的に計算機で解読可能である。この意味で完全な暗号化情報は存在しない。従って、高度の秘匿性を必要とする情報は、インターネットや携帯電話などの通信インフラを利用して伝送することができない。また、高度の秘匿性を必要とする情報を格納するデジタル計算機は、ネットワークへ接続されないか、ファイアウォールと呼ばれるセキュリティシステムを通してネットワークへ接続され、権限のない者によるデータの読み出しや改変等に対するセキュリティを確保している。しかし、ファイアウォールもデジタル計算機で構築されたシステムであるため、デジタル計算機を用いて突破され、いわゆる、ハッキングがなされることを避けがたい。

【0004】 例えば、共用デジタル計算機やネットワークを利用する場合、ユーザ独自のパスワードを正しく入力して初めて以降のアクセス権限が得られるが、この場

合のパスワードは、個々のユーザが持つ暗号解読キーの役割を担うものである。また、デジタル計算機やネットワーク上において、特定のユーザがどの情報へアクセス可能かは、ユーザに与えられた権限に依存する。これは、デジタル計算機を前提とするインターネットや携帯電話等の情報通信と秘匿性の高い情報を格納するデジタル計算機システムにおいて、アクセス権限の階層構造を導入することによって安全性を確保しようとするものである。

【0005】ところが、コンピュータやネットワークの問題とは別に、本来、特定の者がどの情報にアクセス権限を有するべきかという観点から定められるデータへのアクセス権限の階層化と、ネットワーク等の管理の必要性から生じる階層化の要請は、必ずしも同じ内容ではない。例えば、ネットワーク管理者は、ネットワーク上で発生し得る問題の未然防止、発生した問題の解決等を行う関係上、通常、すべてのデータに対してアクセス権限を有するが、これは、企業であれば、ネットワークやコンピュータの専門家であって必ずしも企業の最高責任者でない者が、新製品開発、人事、税務にわたるすべての情報に接しえることを意味しており、データセキュリティの観点からも問題がある。

【0006】このような現状に鑑みると、デジタル計算機を前提とするインターネットや携帯電話等の情報通信と秘匿性の高い情報を格納するデジタル計算機において、ネットワーク管理者も含めた第三者に対する完全なセキュリティを確保することが課題である。他方、組織内では、所属部署、職位に応じて階層的なセキュリティシステムも必要である。

【0007】上記のようなセキュリティ上の問題は、個々のユーザがユーザの所有する全情報を独自に暗号化することで改善される。また、個々のユーザがユーザの所有する全情報を独自に暗号化することは不正ユーザに対するセキュリティの強化となる。しかしながら、全てのユーザがユーザの所有する全情報を独自の暗号で変換する場合、個々のユーザが意図的に情報を暗号化する作業を強いられる点が問題である。また、階層化が必要とされる組織内においては、所属部署、職位に応じて階層的なセキュリティシステムも必要である。

【0008】ここで、階層的とは、ある階層に属するユーザを含めて同じ階層に属するデータにはすべてアクセスできるのみならず、下位の階層に属するデータにはすべてアクセスできるが、上位の階層に属するデータにはアクセスできないようなセキュリティ構成を意味するものとする。ただし、本明細書では、この構成の多くのバリエーションも階層的と称することにする。例えば、特定のユーザに着目した場合、当該ユーザは、同じ階層に属する他のユーザのデータにはアクセス権限をもたないようになることもでき、また、直接の下位のユーザのデータにはアクセス権限があるが、同じ階層に属する他

のユーザに属する下位のユーザにはアクセス権限がないように構成することもできる。

【0009】

【課題を解決するための手段】本発明は、個々のユーザがユーザの所有する全情報を、当該ユーザの個人情報や当該ユーザが任意に設定するデータに基づいて、自動的に暗号化し、公平で、且つ、強固なセキュリティシステムを実現する方法と装置の提案である。すなわち、ユーザが所有する全ての情報をユーザ毎に暗号化し、何れの暗号化情報が秘匿性の高い情報かを、暗号化された情報を解読するまで判断不可能とすることで、セキュリティを高度化すると共に公平なセキュリティ環境を実現する方法である。

【0010】さらに、本発明は、階層化が必要とされる組織において、所属部署、職位に応じて階層的なセキュリティシステムも構成可能とする方法である。すなわち、本発明は、セキュリティを高度化すると共に公平なセキュリティ環境を実現するのみならず階層的セキュリティシステム環境も維持することを可能とする。

【0011】本発明の1側面によれば、ユーザに固有の情報と、ユーザが任意に設定する識別情報の中から選択された1つ以上を組み合わせてキーワードを作成し、該キーワードを用いて少なくとも1つの逆行列を有する適切な行列(well posed matrix)である暗号変換行列を設定し、前記デジタルデータと該暗号変換行列とを積算することによってデジタルデータを暗号化するデータの暗号化方法が提案される。

【0012】本発明の他の側面によれば、前記ユーザに固有の情報は、ユーザの住所、氏名、生年月日、電話番号、ID番号、パスワード、e-mailアドレスの内の少なくとも1つを含むものである暗号化方法が提案される。

【0013】本発明のさらに別の側面によれば、前記のキーワードは、ユーザが独自に決めた任意の組み合わせを選択可能である。

【0014】本発明のさらに別の側面によれば、ユーザが意識することなく、キーワードを用いて自動的に暗号化行列を生成し、ユーザの所有する情報を自動的に暗号化することができる。

【0015】本発明のさらに別の側面によれば、前記暗号変換行列は、单一、若しくは複数の適切な行列の固有ベクトルから生成される单一、若しくは複数のモーダル行列を組み合わせて自動的に生成されたものであり、データを自動的に暗号化する。

【0016】本発明のさらに別の側面によれば、暗号変換行列は、キーワードを用いて、单一、若しくは基底関数の異なる複数のウェーブレット変換行列を用いて自動的に暗号化行列を生成し、ユーザの所有する情報を自動的に暗号化する。

【0017】本発明のさらに別の側面によれば、暗号変換行列は、单一、若しくは複数の適切な行列の固有ベク

トルから生成される单一、若しくは複数のモーダル行列と、キーワードを用いて作成した、单一、若しくは基底関数の異なる複数のウェーブレット変換行列を組み合わせて作成したものである。

【0018】本発明のさらに別の側面によれば、階層ごとに暗号変換行列を設定し、データを当該階層の暗号変換行列及び当該層より下のすべての階層の変換行列を用いて重疊的に変換することにより、上位の階層の属するユーザには当該層及び下位の階層の暗号化データは読めるが、上位の階層の暗号化データは読めない。

【0019】本発明のさらに別の側面によれば、ユーザに固有の情報と、ユーザが任意に設定する識別情報の中から選択された1つ以上を組み合わせてキーワードを作成し、該キーワードを用いて少なくとも1つの逆行列を有する適切な行列 (well posed matrix) である暗号変換行列の逆行列を求め、暗号化されたデジタルデータと該暗号変換行列の逆行列とを積算することによって暗号化されたデジタルデータを解読するデータの解読方法が提供される。

【0020】本発明の別の側面によれば、ユーザに固有の情報と、ユーザが任意に設定する識別情報の中から選択された1つ以上を組み合わせてキーワードを作成部と、該キーワードを用いて少なくとも1つの逆行列を有する適切な行列 (well posed matrix) である暗号変換行列を設定部とを有して、前記デジタルデータと該暗号変換行列とを積算することによってデジタルデータを暗号化するデータの暗号化手段と、前記適切な行列の逆行列を算出する逆行列算出部と、暗号化されたデジタルデータと該逆行列とを積算することによって暗号化されたデジタルデータを解読するデータの解読手段とを有するデータの暗号化解読システムが提供される。

【0021】個々のユーザがユーザの所有する全情報を独自に自動暗号化と暗号化された情報を解読する作業は、暗号化と解読作業の負担をユーザへ強いることのみならずソフトウェア・ハードウェアにも大きな負担がかかる。

【0022】本発明では、ユーザが設定したキーワード、例えばパスワード等、を用いてユーザがセッションを開始した時点で自動的に所望の暗号化テーブルを生成し、ユーザがユーザの所有する暗号化情報へアクセスした時点で、自動的に暗号化テーブル (行列) と暗号化情報 (ベクトル) 間の内積演算で暗号化された情報を解読し、ユーザへ提示する。さらにユーザがセッションを終了する時点で、自動的に暗号化テーブル列 (行) と情報 (ベクトル) 間の内積演算で暗号化された情報を生成し格納することで、ユーザは暗号化・解読作業を意識する必要性が無い。

【0023】本発明における暗号化と解読作業を実施する方法は大別して2つある。一方は、暗号化と解読作業をインタープリター (逐次) 方式で実行する方法であ

り、この方式ではユーザがシステム使用中に當時暗号化テーブルを必要とする。他方は、ユーザがシステムへアクセスした時点で自動的に暗号化テーブルを生成し、ユーザの所有する暗号化された情報を全て解読して提示するバッチ (一括) 方式である。この方式では、暗号化テーブルはセッション開始と終わりにのみ必要とされ、暗号化テーブルを常駐させる必要は無い。

【0024】本発明における暗号化と解読作業を実施するためには、ユーザが設定したキーワードに応じて暗号化テーブルを生成する必要がある。この暗号化テーブルは、暗号化された情報から原情報を完全に復元するため、逆行列が存在する適切な行列であることが必須である。逆行列計算は行列演算の基礎であるため、高速な逆行列演算を可能とするアルゴリズムが多く提案されている。しかし、演算負荷の増加は否めない。逆行列が単純な転置演算で得られるモーダル行列や離散値系直交ウェーブレット変換行列は実質的に逆行列演算を不要とし、ソフト的にもハード的にも演算負荷を最小化し、暗号化と解読作業に必要な演算は、暗号化テーブルの生成と内積演算のみとなる。

【0025】また、暗号化テーブルは、予めユーザが設定したキーワードに応じて複数生成し (請求項7, 8, 9, 10, 11) 、不揮発性メモリーへ書き込んでおき、ユーザがセッション開始した時点で、複数の暗号化テーブルを不揮発性メモリーから呼び出し、行列間の内積演算で実際に使用する暗号化テーブルを生成すれば、演算負荷が低減される。さらに、内積演算専用プロセッサー、例えばDSPチップ (Digital Signal Processor) 等のハードウェアを搭載すれば (請求項12) 、情報処理・情報通信機器本体に対する負担が削減され、ユーザは暗号化と解読作業を事実上意識する必要が無い。

【0026】図1はキーワードから暗号テーブル生成の手順を示し、図2は原情報を暗号化する手順を示す。さらに、図3は暗号化された情報を解読する手順を示す。なお、暗号化テーブルよりも情報のサイズ (行列の次数) が大きい場合、情報のサイズ (ベクトルの次数) を暗号化テーブルのサイズに合わせて分割し、並列演算を行えば大幅な高速化が可能となることや、暗号化テーブルよりも情報のサイズ (行列の次数) が小さい場合、情報ベクトルへ空白やゼロ要素等を適宜追加し、暗号化テーブルのサイズに合わせることは言うまでもない。

【0027】

【発明の実施の形態】

【実施例1】図4はカラーサンプル画像情報の例である。図5はドビッサーの2, 4, 8次基底関数を用いて生成した暗号化テーブルである。図6は図4のカラー画像情報へ図5の暗号化テーブルを適用して暗号化されたカラー画像の赤、緑、青成分情報を示す。図7はドビッサーの2次基底関数を用いて生成した暗号化テーブルを用いて図6の暗号化されたカラー画像情報の解読を試み

て失敗した例である。図8はドビッシーの2, 4, 8次基底関数を用いて生成した暗号化テーブルを用いて図6の暗号化されたカラー画像情報の解読を試みたが、ウェーブレット変換行列の内積演算順序を間違えて失敗した例である。図9はドビッシーの2, 4, 8次基底関数を用いて生成した正確な暗号化テーブルを用いて図6の暗号化されたカラー画像情報の解読に成功した例である。

【0028】

【実施例2】図10は半角アルファベットのサンプルテキスト情報の例である。図11は図10の半角アルファベットで書かれたテキストのアスキーコード表示である。図12は2階偏微分方程式を3点有限差分公式で離散化したシステム行列のモーダルマトリックスから生成した暗号化テーブルである。図13は図10に示すテキスト情報を図12の暗号表を用いて暗号化した例である。

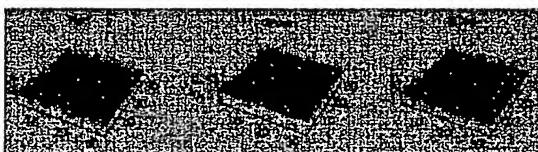
【0029】

【実施例3】図14は日本語全角のサンプルテキスト情報である。図15は図14のサンプルテキスト情報を図12の暗号化テーブルを用いて暗号化した例である。図16は図15に示す暗号化されたテキスト情報を解読した例である。

【0030】

【発明の効果】実施例1から明らかのように、図5に示した複数のウェーブレット変換行列を組み合わせた暗号化テーブル（変換行列）を用いた線形変換で、図4に示したサンプルカラー画像情報を図6へ示した暗号化されたカラー画像情報へ変換できる。また、図7と図8に示したように、キーワードから決まる暗号化テーブルを使用しなければ、暗号化されたカラー画像情報は解読できない。実施例2と実施例3に示したように、半角文字であれ全角文字であれ暗号化が可能である。暗号化された文字情報は、キーワードから決まる暗号化テーブルを使用しなければ解読不可能である。拠って、本発明は、個々のユーザがユーザの所有する全情報を独自に自動的に暗号化し、公平で、且つ、強固なセキュリティシステム実現する方法と装置の提供する。また、暗号化テーブルを生成するモーダル行列やウェーブレット変換行列の組み合わせを限定すれば、階層的な暗号化システムを構築可能であることは言うまでも無い。

【図6】



【図面の簡単な説明】

【図1】 図1は、キーワードによる暗号化手順である。

【図2】 図2は、暗号化手順である。

【図3】 図3は、暗号化された情報を解読する手順である。

【図4】 図4は、カラーサンプル画像情報の例である。

【図5】 図5は、ドビッシーの2, 4, 8次基底関数を用いて生成した暗号化テーブルである。

【図6】 図6は、図4に示したカラー画像情報へ図5に示した暗号化テーブルを適用して暗号化したカラー画像の、赤、緑、青成分情報である。

【図7】 図7は、ドビッシーの2次基底関数を用いて生成した暗号化テーブルを用いて図6の暗号化されたカラー画像情報の解読を試み失敗した例である。

【図8】 図8は、ドビッシーの2, 4, 8次基底関数を用いて生成した暗号化テーブルを用いて図2(c)の暗号化されたカラー画像情報の解読を試みたが、ウェーブレット変換行列の内積演算順序を間違えて失敗した例である。

【図9】 図9は、ドビッシーの2, 4, 8次基底関数を用いて生成した暗号化テーブルを用いて図6に示した暗号化カラー画像の解読に成功した例である。

【図10】 図10は、半角アルファベットのサンプルテキスト情報の例である

【図11】 図11は、図10の半角アルファベットで書かれたテキストのアスキーコード表示である。

【図12】 図12は、2階偏微分方程式を3点有限差分公式で離散化したシステム行列のモーダルマトリックスから生成した暗号化テーブルである。

【図13】 図13は、図10のテキストを図12の暗号表を用いて暗号化した例である。

【図14】 図14は、日本語全角文字で書かれたサンプルテキスト情報である。

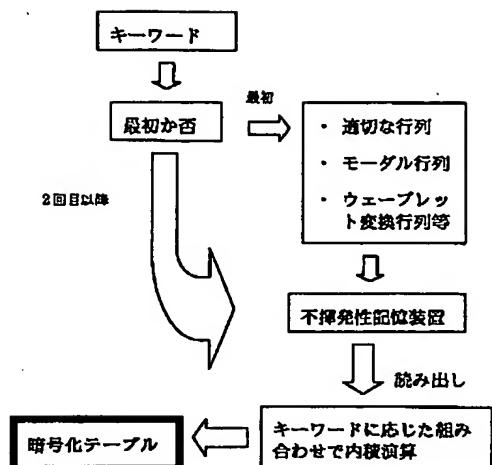
【図15】 図15は、図14のサンプルテキスト情報を図12の暗号表を用いて暗号化した例である。

【図16】 図16は、図15の暗号化情報を解読した例である。

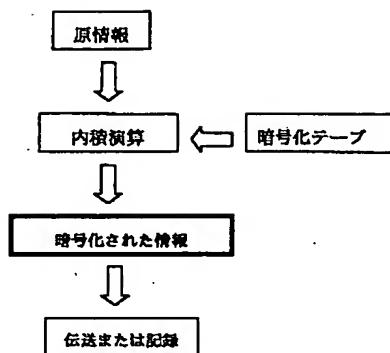
【図10】

"abcdefghijklmnopqrstuvwxyz012345678"

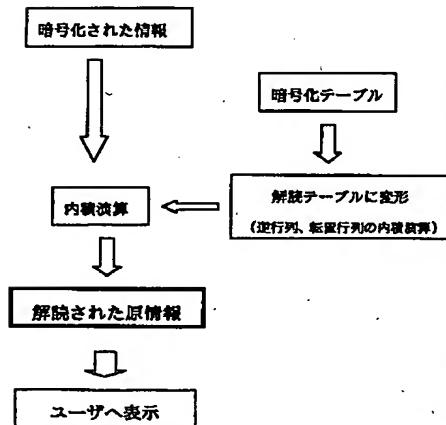
【図1】



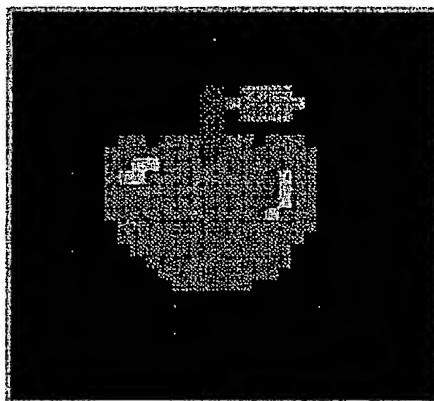
【図2】



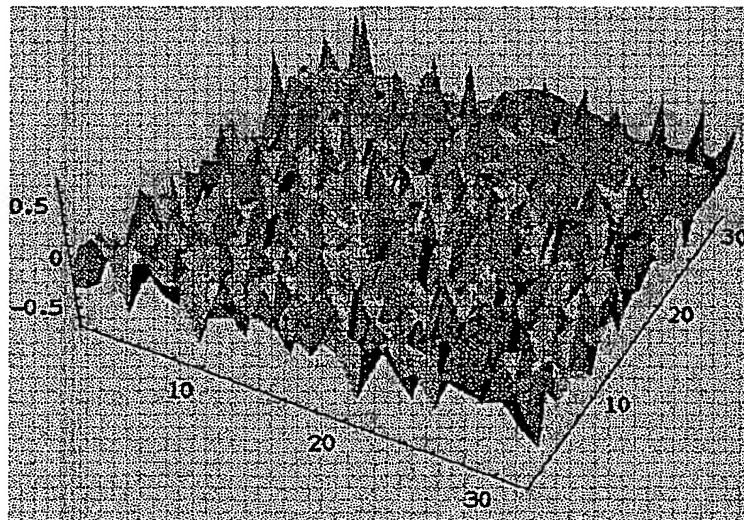
【図3】



【図4】

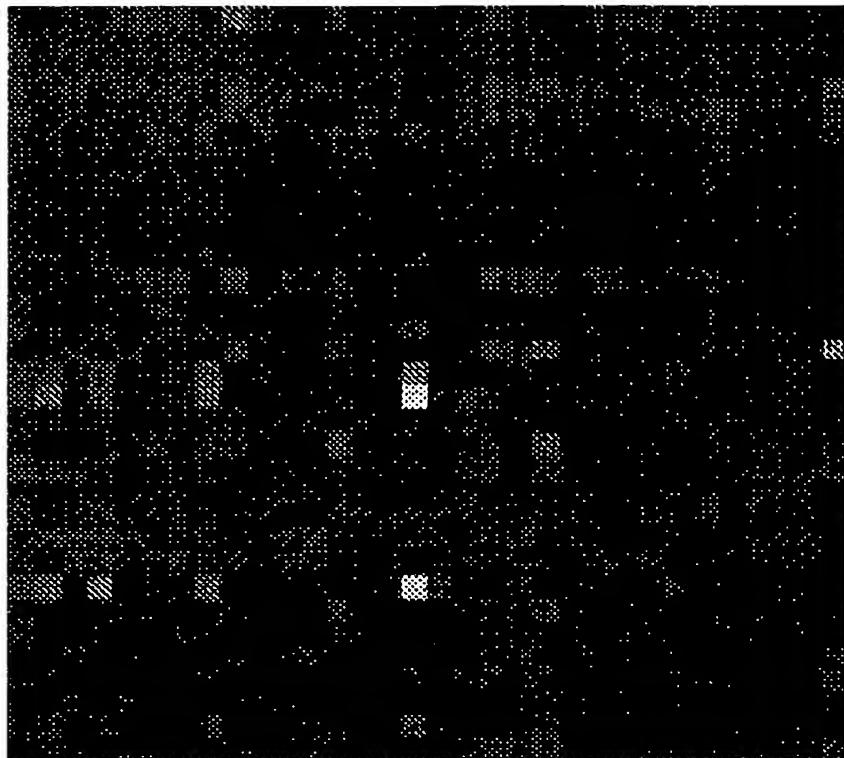


【図5】

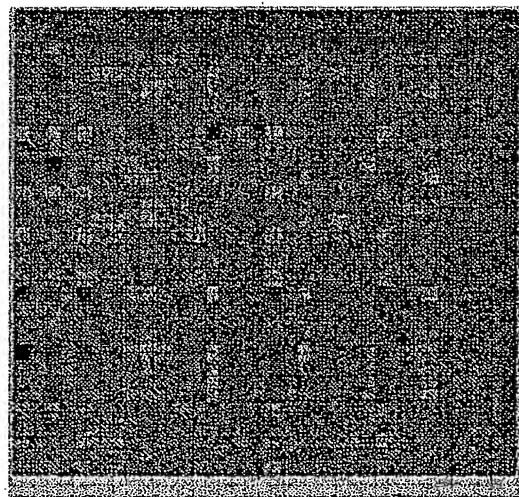


BEST AVAILABLE COPY

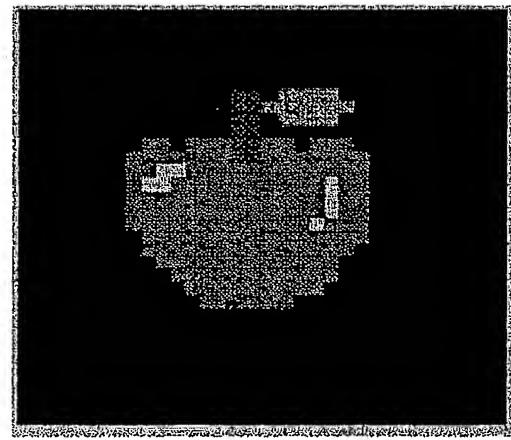
【図7】



【図8】



【図9】

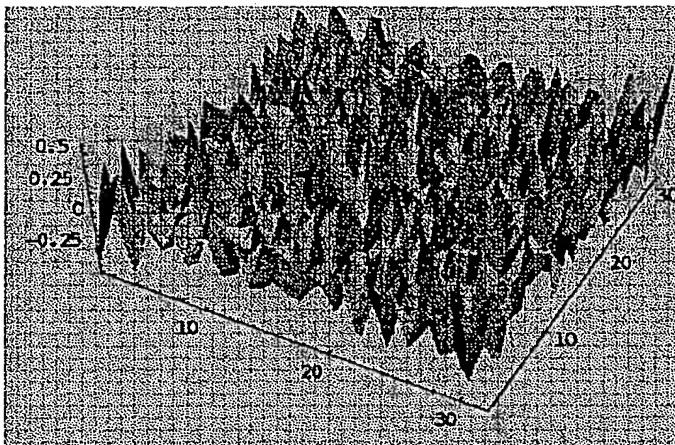


【図11】

97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111,
112, 113, 114, 115, 116, 117, 118, 119, 48, 49, 50, 51, 52, 53, 54, 55, 56

BEST AVAILABLE COPY

【図12】



【図16】

皆さん、 こんにちわ、 何とか日本語でも暗号化可能なコードを開発しました。 これからはこの暗号化システムで文書のやり取りをしましょう。

【図13】

-8.74191, 39.7368, 87.6053, 94.0775, 12.8818, -76.4189, -72.2557, 52.0616, -36.6965, 77.0434, 62.4916, 131.028, 34.1975, 28.3981, -179.044, -51.3442, 132.441, -28.3465, -83.7825, -143.01, -106.561, -168.017, -121.319, -89.9274, -82.5656, 182.661, 135.088, -24.1645, -1.19803, 169.481, 24.2129, 2.28735

【図14】

皆さん、

こんにちわ、

何とか日本語でも暗号化可能なコードを開発しました。
これからはこの暗号化システムで文書のやり取りをしましょう。"

【図15】

```
{48190.79823062123, -6319.637283039465, 19346.461652865546, 12433.958434272141, 21524.08996836047, 24797.108744101988, -18514.820246008177, 16013.687026444268, 30265.0553055384, -6497.465630124796, 13599.260456776039, -26315.488304357154, -2883.8173409195433, -5023.767076496519, -12333.48401262003, 15249.522440238332, -28314.8842262108, -10386.071518507144, 2848.025787245269, 49095.34436022277}, {-17781.53107610992, -9235.781799446671, 16200.682818526391, -10795.583352919595, 6411.002877304985, -969.4490598252514, 13209.018761450818, -9564.471169455757, 317.09530806134836, 2300.040585386563, -3227.7495536456395, 18908.102460502647, 13910.329919723792, -28.100380578100005, 8378.756146292453, 561.1142031880618, 231.8466781773551, 24994.89231171991, -12340.33719400903, -1.5753.458742717527}, {41776.4594638209, -8267.22926557176, 15807.95800409425, 2290.8526118224213, 1717.901752975521, 27811.266310507523, -9318.783980232633, 9068.08720634938, 21411.03803886653, 2091.820731914362, 1743.7243656264188, -4306.921764061262, 6350.015061950382, -5611.746636792715, -16885.14831471636, 5861.345679751021, -7141.341462214608, 7989.338040335448, -2202.5100587241714, 21903.338262517227}, {16937.607580944485, -24551, -2284.2191725007765, 870.3131615394636, 10898.340027007604, -8684.157083568927, 1931.8866202388288, 3476.1034717325283, 14772.281093752617, -708.0719377731511, -18235.726824067402, 7933.00691288516, -8852.366573788604, 1169.9868798606221, -4352.399593458086, 25301.21571070453)
```